仕 様 書

1. 件名

WEB アプリケーションファイアウォールの購入

2. 数量

1 式

3. 目的

近年は WEB サーバの脆弱性を利用したサイバー攻撃が急増しており、多くのインターネット上の公開 WEB サイトが、情報の改ざん、情報漏洩などの被害を受けている。本機器は、これらのサイバー攻撃から WEB サーバを保護するための専用機器であり、本研究所が外部に情報を公開している WEB サイト環境に導入することで、公開 WEB サイトの安全性を強化する。

4. 納入期限

平成 28 年 2 月 29 日

5. 納入場所

放射線医学総合研究所
重粒子治療推進棟地下 1 階ネットワークサーバ室

6. 構成

(1)	WEB アプリケーションファイアウォール	1 台
(2)	管理装置	1 台
(3)	設置設定作業	1 式

7.　仕様・性能

(1) WEBアプリケーションファイアウォール

以下の仕様を満たすWEBアプリケーションファイアウォール(以下「WAF」という。)を納入すること。

1) WAF機能に特化したアプライアンス製品であること。

2) 「図1 WAFの概要」に示すインライン配置(ブリッジ配置)が可能であり、導入の際に、既設ネットワーク機器等のIPアドレス変更が不要なこと。

3) 100BASE-TX及び1000BASE-Tに対応したネットワークインターフェースを4ポート以上有し、「図1 WAFの概要」に示す2系統のネットワーク(DMZ-1,DMZ-2)を防御可能なこと。

4) 本機器が障害等により停止した場合、インライン配置用ネットワークインターフェースを自動的にバイパスし、WAF機能が無効になった状態で通信を維持できるイーサネットバイパス機能を有すること。また、同イーサネットバイパス機能は、設定により有効・無効を切り替えられること。

5) WAF機能のHTTPスループットは、本機器全体で500Mbps以上であること。

6) 以下の防御機能を有すること。

A) 「図1 WAFの概要」に示す攻撃の検知・防御が可能なこと。

B) 攻撃の検知方法は、ブラックリスト方式及びホワイトリスト方式に対応しており、防御対象のWEBサイト毎に検知方法を変更可能なこと。

〇ブラックリスト方式
既知の攻撃パターンを検知するシグネチャを利用し、同シグネチャに合致したものを攻撃と判断する方式。
〇ホワイトリスト方式
正規の利用パターンをリスト化し、同リストに合致しないものを攻撃と判断する方式。

C) SQLインジェクションやクロスサイトスクリプティングに特化した相関分析ルールによる攻撃の検知が可能なこと。

D) ブラックリスト方式で利用するシグネチャは、新たな攻撃パターンが発見された際に製造元等によりに更新され、本機器に自動的に反映されること。

E) 稼働中の通信内容を基にして、適切なホワイトリストを自動作成する機能を有すること。

F) HTTPS(SSL/TSL)によって暗号化されたWEBサイトの防御に対応しており、暗号処理によるスループット低下を防ぐためのSSLアクセラレータ用ボード等を内蔵していること。また、暗号処理は、ワイルドカードサーバ証明書に対応していること。

7) 以下のログ・通知機能を有すること。

A) 検知した攻撃のログを「(2)管理装置」に記録可能なこと。また、管理装置への記録と並行して、SYSLOGサーバへ転送することが可能なこと。(本契約に

SYSLOG サーバの調達は含まない。)

B) 攻撃を検知した際に、指定した電子メールアドレスに通知する機能を有すること。

8) 「(2)管理装置」との接続用として、100BASE-TX 又は 1000BASE-T に対応したネットワークインターフェースを有すること。

9) EIA 規格 19 インチラックに搭載可能であり、高さは 2U 以下であること。

10) 本体の奥行きは、80cm 以下であること。

11) 商用電源 100V/50Hz での動作が保証されていること。

(2) 管理装置

以下の仕様を満たす管理装置を納入すること。なお、同管理装置は、内部ネットワークに設置するため、WAF 本体とは独立していること。

1) 本契約で導入する WAF の設定・管理及びログの閲覧等を WEB インターフェースから行えること。

2) WAF が出力したログを集計し、時毎、日毎、WEB サイト毎の攻撃を集計したレポート(PDF 形式)を作成する機能を有すること。また、同レポートを定期的に自動作成し、指定した電子メールアドレスへの送信が可能なこと。

3) EIA 規格 19 インチラックに搭載可能であり、高さは 1U 以下であること。

4) 本体の奥行きは、80cm 以下であること。

5) 商用電源 100V/50Hz での動作が保証されていること。
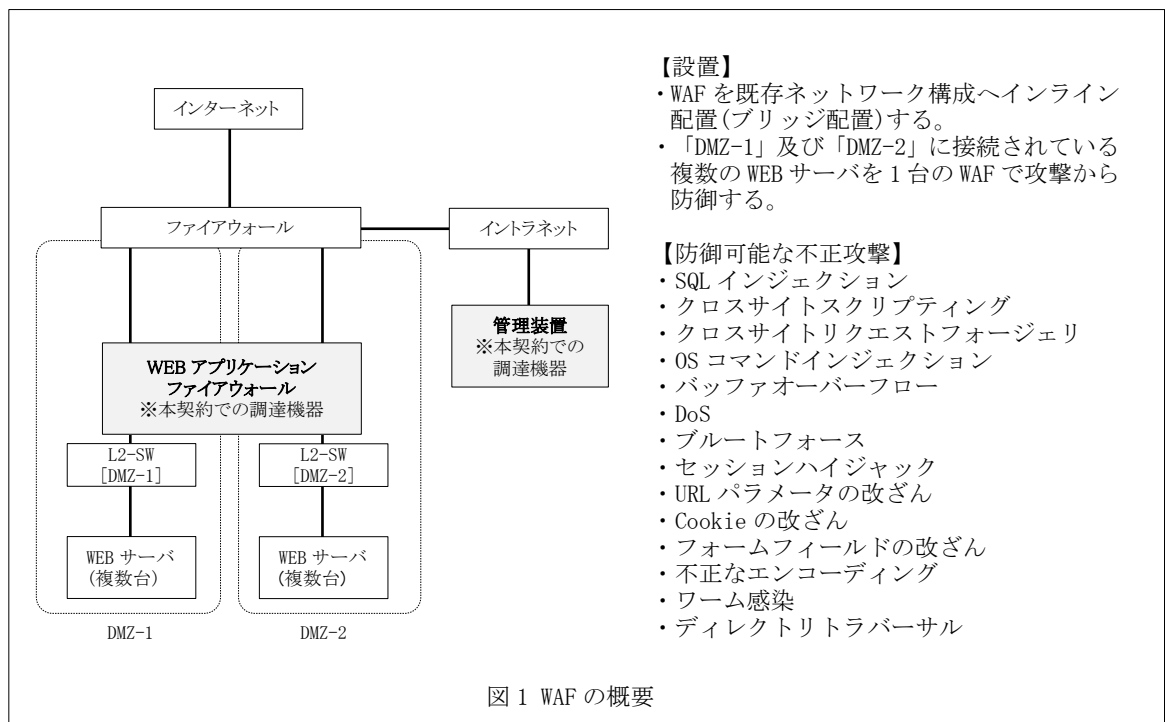
図 1 WAF の概要

(3) 設置設定作業

以下の設置設定作業を行うこと。

1) WAF を既設 EIA 規格 19 インチラックに設置すること。なお、設置に必要な金具等は受注者が用意すること。

2) WAF の電源は、当研究所が指定する電源コンセント(NEMA5-15R)からとること。

3) WAF をネットワークに接続するケーブルは、当研究所が用意する。本契約に LAN 工事は含まない。

4) 「図 1 WAF の概要」に示す防御動作が可能なように WAF を設定すること。なお、防御についての詳細な設定・調整を行う WEB サイトは、DMZ-1 に設置された 1 サイトのみとする。

5) 設定の詳細については、当研究所担当者と協議上で決定すること。

8. 提出図書

以下の図書を提出すること。

1) 導入機器の設定情報(紙媒体及び電子媒体を各 1 部)

2) 導入機器の取扱説明書

9. 検査

当研究所職員が所定の要件を満たしていることを確認したことをもって検査合格とする。

10. その他

1）本契約で調達する機器の保守については、本契約に含まないものとする。

2）管理者向けの操作説明会を１回開催すること。なお、説明内容には、新規に WEB サイトを防御対象として登録するための手順を含むこと。

3）本仕様を満たすためにソフトウェアライセンス等(ブラックリスト用シグネチャの利用ライセンスを含む。）が必要な場合、納入から３年分のライセンスを本契約に含めること。

4）本契約においてグリーン購入法に適用する環境物品が発生する場合は、原則として、それを採用すること。

5）本契約の実施により知り得た情報を許可なく第三者に洩らしてはならない。

6）本仕様書の内容について疑義が生じた場合、又は本仕様書に規定のない事項については別途協議の上決定する。

（要 求 者）

部課名：研究基盤センター 情報基盤部
情報基盤システム課

氏　名：佐藤　眞一郎